Exhibit K

Apple Bank for Savings Member FDIC	**Acceptable Use Policy**
	CONFIDENTIAL

1.0 Overview

The most common reasons to provide an user access to the Bank information technology resources is for granting access to employees for the performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the Bank information technology resources.

The intent of this policy is not to impose restrictions but to provide protection of the Bank, its affiliates, officers, employees, consultants and vendors from illegal or damaging actions by individuals, either intentional or not intentional.

Security of the Bank's information technology resources is a team effort involving the participation and support of every Apple Bank user. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Any questions on what constitutes acceptable use should be directed to the user's immediate supervisor/manager.

2.0 Purpose

The purpose of this policy is to provide guidelines for the acceptable use of Apple Bank information technology resources. These guidelines are in place to protect all parties involved. Inappropriate use of Bank information technology resources exposes the Bank to potential risks including virus attacks, compromise of network systems and services and legal issues.

3.0 Scope

This policy applies to the use of Bank information technology resources to conduct Apple Bank business or interact with internal networks and business systems, whether owned or leased by Apple Bank, the employee, or a third party.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Apple Bank, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Apple Bank.

4.0 Policy

4.1 General Use

All users of Bank information technology resources must comply with Bank policies, standards, procedures, and guidelines, as well as any applicable Federal, State and local laws, including intellectual property rights, laws governing trademarks, copyrights, trade secrets as well as the particular requirements of the applicable licensing agreements.

While Bank's network administration desires to provide a reasonable level of privacy, users should be aware that anything created on Bank information technology resources remains the property of Apple Bank. Because of the need to protect Apple Bank network, management cannot guarantee the confidentiality of information stored on any of Bank information technology resources.

Periodic monitoring and reviews may be conducted of all Bank information technology resources, including but not limited to all computer files and all forms of electronic communication, including e-mail.

You may access, use or share Apple Bank sensitive information only to the extent it is authorized and necessary to fulfill your job responsibilities.

Users accessing Bank information technology resources and/or applications through the use of personal devices must only do so with prior approval from the Chief Technology Officer and the Chief Information Security Officer.

4.2 Security

Individual accountability is required when accessing all Bank information technology resources. Each individual is responsible for protecting his or her available resources against unauthorized activities performed under their user account.

All PCs, workstations and servers should be secured when left unattended for extended period of time or at the end of the day. This can be accomplished by a password-protected screensaver, logging-off (control-alt-delete) or shutting down.

Keep passwords secure and do not share user accounts. Users are responsible for the security of their passwords and accounts; they must be treated as strictly confidential information and must not be disclosed or shared.

The Bank may impose restrictions, at the discretion of senior management, on the use of a particular information technology resource. The Bank may block access to certain websites or services not serving legitimate business purposes or may restrict users' ability to attach devices to the Bank's information technology resources (e.g., external storage devices, external hard drives).

All users have a responsibility for protecting sensitive information from unauthorized use or disclosure and observing authorized levels of access and utilizing only approved information technology devices or services.

Avoid transmission of sensitive information. If it is necessary to transmit sensitive information, employees are required to take steps reasonably intended to ensure that information is encrypted and is securely delivered to the proper person who is authorized to receive such information for a legitimate use.

4.3 Unacceptable Use

The following actions shall constitute unacceptable use of the Bank information technology resources. Some employees may be exempted from these restrictions during the course of their legitimate job responsibilities (systems administration tasks, security investigations, etc.).

This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable.

- Copying, storing and/or transferring any Bank related information by any means that is not expressly authorized herein.
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate.
- Copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Apple Bank or the end user does not have an active license.
- Accessing data, a server or an account for any purpose other than conducting Bank business, even if you have authorized access.
- Connecting non-bank provided equipment/devices to the Bank network or any Bank information technology resource.
- Connecting Bank information technology resources to unauthorized networks.
- Connecting to any wireless network while physically connected to a Bank network.

- Connecting to commercial e-mail systems (e.g., Gmail, Windows Live, etc.) without prior management approval (There is an inherent risk in using commercial e-mail services as e-mail is often used to distribute malware).
- Installing, downloading, or running software or code that has not been supplied by the Bank and/or approved by the Bank.
- Installing or distributing unlicensed or "pirated" software.
- Revealing passwords or providing unauthorized third parties, including family and friends, access to the Bank information technology resources or facilities.
- Excessive use of Bank bandwidth or other computer resources. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low bank-wide usage.
- Purporting to represent Apple Bank in matters unrelated to official authorized job duties or responsibilities.
- Using Bank information technology resources to circulate unauthorized solicitations or advertisements for non-bank purposes including religious, political, or not-for-profit entities.
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using Bank information technology resources.
- Using B a n k information technology resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Using Bank information technology resources to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly tampering, disengaging or otherwise circumventing Apple Bank or third-party IT security controls.
- Using Bank information technology resources for instant Messaging, peer to peer file sharing and streaming media.

4.4 E-Mail

Users need to exercise common sense when sending or receiving e-mail from the Bank e-mail accounts. Users need to recognize that e-mails sent from a Bank e-mail account reflects on the Bank and, as such, e-mail must be used with professionalism and courtesy.

Users must use extreme caution when opening e-mail attachments received from unknown senders, these attachments may contain viruses, malware, Trojan horse code, etc.

In addition to the prohibited actions set forth as "Unacceptable Use" at section 4.3, above, the following actions are also prohibited:

- E-mailing any Bank related "sensitive" information over any channel not encrypted.
- E-mailing any Bank related information to your home or any third party or person not authorized to access such information.
- Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
- Any form of harassment whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of e-mail header information.
- Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited e-mail originating from within Bank's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Bank or connected via Bank's network.
- Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

4.5 Social Media

Apple Bank reserves the right to establish corporate presences in its name on any other social media site. Marketing and Executive Management will determine when and if such presences are in the interest of the Bank. Marketing is the only group authorized to create these presences.

Employees who create a personal presence within a social media site and who choose to identify themselves as an Apple Bank employee must act in accordance with the Bank's web guidelines as follows:

Engage in Good Web Communication Practices. When communicating with others through social media sites, Apple Bank employees who identify themselves as such must maintain the same standards of professionalism and accuracy as they would in a person- to-person meeting at a bank office or a telephone conversation with a customer or prospect. Employees must not post derogatory, profane or defaming comments or opinions about the Bank or other Bank employees. Employees should avoid unprofessional slang, communicate clearly, and avoid opinions about, or links to sites discussing religion, politics or other controversial topics

Refer product and service questions to the Bank's website www.applebank.com and refer new media and other questions to Marketing.

4.6 Personal Usage

Personal usage of Bank information technology resources is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the Bank or on the user's job performance.

Users should be guided by department policies on personal use and for exercising good judgment regarding the reasonableness of personal use. If you are unclear about the acceptable "personal" use of Bank information technology resources, consult your immediate supervisor/manager.

4.7 Remote Desktop Access

Use of remote desktop software and/or services is allowable as long as it is provided by the Bank.

For more detail information, refer to the Apple Bank's Remote Access Policy.

4.8 Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor/manager. For more detail information, refer to the Apple Bank's Incident Response Plan. Some examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/ransomware.
- Loss or theft of any device that contains Bank information.
- Loss or theft of ID card or keycard/keydevice.
- Any attempt by any person to obtain a user's password over the telephone or by e-mail.
- Any other suspicious event that may impact the Bank's information security.

4.9 Applicability of Other Policies

This document is part of the Bank's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Compliance

The Chief Information Security Officer (CISO) will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the Chief Information Security Officer/designated individual in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions of Key Terms

Information Technology Resources - Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, e-mail, and social media sites.

Instant Messaging - is a type of online chat that offers real-time text transmission over the Internet.

Peer-to-Peer (P2P) File Sharing - A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Sensitive information - Information that is of the most utmost corporate sensitivity, intended exclusively for executive level distribution and/or is considered critical to the organization's on-going operations and could seriously impedes the Bank if made public or shared internally. This could include information on pending mergers, acquisitions, product development or investment strategies, business plans, accounting information, network information, customer information protected by state laws, federal regulations (e.g., Gramm-Leach- Bliley), statutes, executive orders and information protected by Bank policy or contracts.

Customer information would include a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that

would permit access to the customer's account. Credential or session information that can be used to access this information would also be included.

Streaming Media - is multimedia that is constantly received by and presented to an end-user while being delivered by a provider, typically audio and/or video. The user can start playing a clip before the entire download has completed.

***7.0 User Agreement** (to be signed by user)*

- I have read and understand the Acceptable Use Policy.
- I am aware that anything created using Apple Bank information technology resources is and shall remain the sole property of Apple Bank.
- I am aware periodic monitoring and reviews of Apple Bank information technology resources may be conducted, including but not limited to analyses of all my computer files and electronic communications, in any form, including my e-mail account(s).
- I acknowledge that I have no reasonable expectation as to individual privacy or confidentiality with regard to any and all of the Apple Bank information technology resources that I use or to which I have access, now or hereafter.
- I will access, use or share Apple Bank sensitive/confidential information only to the extent it is expressly authorized by the Bank and necessary to fulfill my job responsibilities, on a need to know basis.
- I understand that upon any violation of this Acceptable Use policy I may be subject to disciplinary action by the Bank, up to and including termination of employment.
- By signing below, I consent and agreeing to the conditions of the Acceptable Use Policy for Apple Bank.

Ricardo F. Mazzitelli
User Name (print)

GRC Risk Solutions
Company Name (print)

X
User Signature

9/11/2017
Date